Litton
PRC

PRC•PRéCis™

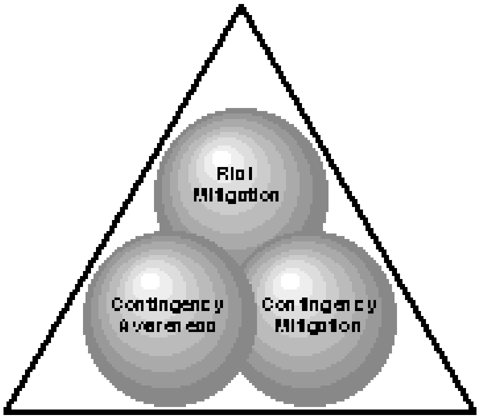
"provides concise summaries of audits in your network environment"

Background

PRC•PRéCis™ is a toolkit that automates all aspects of audit processing in a network environment. The goal of this toolkit is to alleviate the tedious work associated with processing audits and deriving useful information from them. Audit processing activities are essentially placed in "autopilot mode", with manual intervention required only when the situation warrants. The purpose of the PRéCis toolkit is to:

- Provide an infrastructure to identify security events as they occur in the network
- Provide the Security Officer with notification that a security event is ongoing
- Provide the means to assess damage after the fact
- Act as a deterrent to would-be perpetrators.

The suite of automated tools in the toolkit provides you with the means to implement a comprehensive security policy for your network. The purpose of a security policy is to protect valuable information assets from compromise. PRC views comprehensive network security policy as a triad, consisting of risk mitigation, contingency awareness, and contingency mitigation, as illustrated below.



Risk mitigation policy alone can provide safeguards and administrative procedures designed to make it difficult for information to be compromised. However, since information resources are always subject to attack and compromise, regardless of the measures taken to enhance the safeguards, contingency policies are vital to an effective security policy. Contingency policies will help you identify when a compromise takes place and what information may have been compromised.

Solutions for Difficult Problems

With the ability to consolidate and analyze network audits from all audit sources in the network, the PRéCis toolkit allows you to achieve an effective balance in your overall security policy by supplementing risk mitigation policy with contingency policies. With the PRéCis toolkit, you can readily determine whether your information assets have been compromised and you are provided with the means to deal with a compromise after it has taken place. With these tools, you can realize substantial cost savings by eliminating labor intensive procedures needed to implement that policy.

The PRéCis toolkit provides you with concise summaries of audit information at many levels, including:

- Near real-time security *alerts* (defined by your policy) triggered by specified user actions;
- Near real-time alerts generated by an inferential analysis capability that aggregates multiple indicators and anomalies that might not appear suspicious when considered separately;
- Near real-time viewing of audits generated by a single user or a single machine;
- Distilled summaries of user activities in statistical format;
- Distilled summaries of user activities in a common, normalized audit format;
- Detailed summaries of user activities in native audit format (also known as raw audits); and
- Ad hoc or standing query methods for report generation.

The PRéCis toolkit also provides a deterrence to anyone wishing to compromise your information assets. If a person wishing to do so is aware that your organization possesses the means to identify a compromise and provide supporting evidence for a prosecution, there is less likelihood that person would undertake those actions.

There are many barriers preventing an organization from dealing effectively with information compromise. The PRéCis toolkit breaks down those barriers and provides a comprehensive set of tools needed to deal with them. Each of these barriers is a problem set requiring solutions.

Audit Generation:

Because audits generated by operating systems tend to be at a very low level (machine operations, as opposed to human operations), they can represent a large volume of data and can be a burden on day-to-day operations. Your organization may be reluctant to commit the resources to deal with audits because there are no means for efficiently collecting and archiving the data. However, audits represent a useful means of recording evidence of user activities on a computer. Without audit information, there is little chance a compromise will be detected and little chance that a perpetrator will be prosecuted.

The PRéCis toolkit offers solutions for this problem set by providing the means to manage audits once they are generated. Choosing to activate audits will then become an easier decision for your organization to make.

Audit Archive:

Audits must be protected and preserved in the original, unaltered format, if there is to be any chance for proving that an individual has compromised information. Because of the great volume of these audits, they can not ordinarily be maintained on-line for long periods or until all potential analysis activities are completed. Audit analysis activities might need to be accomplished many weeks after the audits are generated. The analysis effort must be able to locate supporting audits wherever they may be—at the audit source, on-line at a central location, or archived on long-term storage.

The PRéCis toolkit offers solutions to this problem set by providing comprehensive archiving facilities and a means of indexing back into the archives. A unique feature of the toolkit is our *Virtual Storage* concept, permitting audit tools to access archived native audits as if they were stored in on-line files. Thus, there is no compelling reason to store a large volume of native audits on-line, since they are readily accessible once they are archived. You need only the most recent native audits on-line to perform your routine analysis activities. After that, archives will typically be accessed only when examining a special circumstance in greater detail, possibly after considerable time has elapsed.

Audit Integration:

In a network environment, user activities can span several network nodes. To effectively assess user behavior in this environment, it is necessary to integrate audits from multiple sources. This can be accomplished by placing audits into a relational data base for analysis purposes. However, in a multi-vendor network environment, machines produce audits in multiple, dissimilar formats, making it difficult to meaningfully integrate native audits into a data base. Audits are best integrated by converting them into a common, normalized representation before placing them into a data base.

The PRéCis toolkit offers solutions to this problem set by normalizing native audit records from multiple network source nodes and placing them into an Audit Analysis data base. The PRéCis toolkit is able to correctly sequence normalized audits chronologically, even if the clocks on each audit source are widely variant. This *Delta Time* feature facilitates analysis of user activities spanning multiple network nodes.

Audit Volume Reduction:

The low-level nature of native audits means that information describing user activities is represented by a much larger set of audits than is really necessary for analysis purposes (i.e., a single log-on can generate in excess of 100 low level audits). For audit integration, it is not enough to simply convert audits into a normalized form so they may be integrated into a data base. The data base size would be too large to be effective. Integration must be accomplished by eliminating unnecessary audits *before* they are integrated into a data base.

The PRéCis toolkit offers solutions to this problem set by providing for *rule-based audit reduction* capabilities that can reduce the audit volume by as much as 90%. The reduction algorithms are tailorable, so that an organization may customize the process to suit their requirements.

Alert Generation:

An important function required for implementing a contingency awareness policy is to have the capability to screen audits as they are generated, looking for designated events that represent exception conditions that need to be brought to the attention of the Security Officer.

The PRéCis toolkit offers solutions to this problem set by providing the capability to detect alerts at the audit source and have the alert information directed to an alert monitoring window at the Security Officer's workstation. With PRéCis tools, the definition of alerts is tailorable, so that your organization may choose to highlight information that is relevant to your requirements.

Audit Analysis:

The key to learning whether information assets have been compromised is to have the capability to perform an automated analysis of the audits. For this purpose, native audits are ineffective and of little use. First-level analysis is best done with normalized audits.

The PRéCis toolkit offers solutions to this problem set by providing analysis tools that operate with normalized audits. These tools provide the means for a first-level analysis of any situation. Normalized audits in the analysis data base support day-to-day analysis efforts with query and reporting capabilities. For rule-based interpretation of audit activity in near-real time, normalized audits may be fed to the rule-based anomaly detection component of the PRéCis toolkit. Statistical summaries are also produced by this analysis.

Situation Analysis:

When your audit analysis has determined that information compromise has taken place, it must be possible to relate the information used in the analysis effort to the actual information contained in the native audits. (Derived audit information like normalized audits is not sufficient legal evidence for prosecution.) It must also be possible to query the native audit archives to readily locate the actual audit information that supports the audit analysis effort.

The PRéCis toolkit offers solutions to this problem set by providing a link mechanism from the normalized audits back to the native audits that were originally mapped into the normalized audits. The toolkit also provides a query tool to provide access to archived native audits, using the *Virtual Storage* facility. In the event that a situation is on-going, the toolkit also offers the capability to monitor audits from a single user or a single machine in near-real time as the activities take place.

Audit Management:

Audits generated in near real-time present control issues. Audit files could overflow and collection nodes might be taken off line for maintenance. An effective audit environment must have the means to manage audit flows and audit levels. If audits are not effectively managed, data might be lost and be unavailable to support audit analysis and prosecution analysis. The PRéCis toolkit offers solutions to this problem set by providing tools to configure and manage audit operations.

Product Description

When your organization wishes to adopt security policies that deal with a contingency situation, you need tools that can provide you with awareness that a contingency has occurred (or is in progress). You also need tools to support analysis activities necessary to discover exactly what might have been compromised and who the perpetrator might be. These same tools must also support daily or periodic monitoring and analysis activities. These tools are part of the PRéCis toolkit.

The PRéCis tools support operations in small or large, multi-vendor networks. In a network environment, activities leading to information compromise can occur on several network nodes in tandem. If activities on single network nodes are examined in isolation, there is a chance that compromising activities may not be detected. Thus, audits from all audit sources in the network must be gathered and preserved in order to provide evidence of information compromise or misuse. In a multi-vendor, open systems network environment, the native audits are generated in many different formats. These must also be transformed into a common, normalized form and then consolidated in order to derive useful information from audit analysis activities. The PRéCis toolkit provides the tools to support these capabilities.

The PRéCis toolkit provides an open framework for tools supporting the contingency awareness and contingency mitigation functions of an overall security policy. The suite of tools provided with the toolkit are all available to the Security Officer with an integrated interface, operable from a single network workstation. The Security Officer is provided with:

- Tools with which to process audits;
- Facilities for archiving native audits;
- Tools for monitoring the security status of the network;
- Tools for performing audit analysis and reporting; and
- Tools for configuring and administering the network audit environment.

Audits generated in the network environment serve two purposes. First, native audits represent machine-level tokens of user activities and can be used to relate user activities to an information compromise situation after the fact. The PRéCis toolkit provides facilities for collecting and archiving these native audits so that they may be utilized later, if needed. Second, audits can be used to perform analysis of user activities in order to determine whether undesirable or unauthorized activities are present in the network.

Because native audits are voluminous and contain unnecessary information about system-level activities, they are not well suited for audit analysis activities. Therefore, the PRéCis toolkit provides facilities for converting native audits into a normalized representation, which greatly reduces the audit volume, while facilitating meaningful audit analysis. Normalized audits are consolidated into a single audit analysis data base, which can then be used to support audit analysis tools. PRéCis provides support for transporting native audits and normalized audits, in bulk mode or in near real-time mode, between network nodes using TCP/IP protocol.

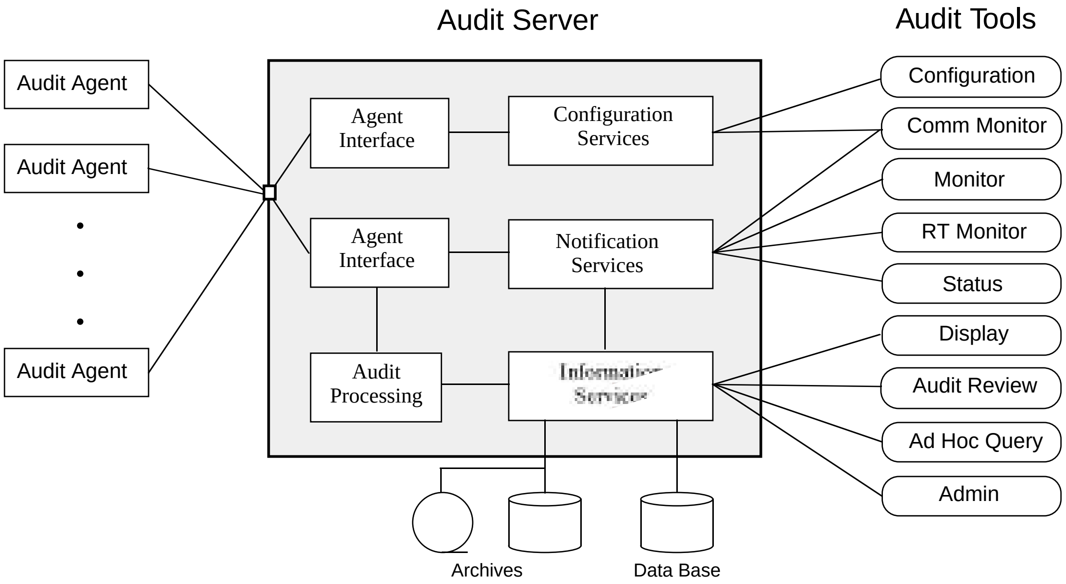
The common format used for normalized audit representation is the *eXtended Host Audit Collection* (XHAC) format. The XHAC format is an object-oriented format that reduces the number of distinct audit events to the lowest common denominator, while preserving the descriptive event information as additional fields in the record. The XHAC format includes B-level audit events as well as C-level audit events.

Software Architecture

The PRéCis software architecture, illustrated in the figure below, includes a central Audit Server component, a set of Audit Tools, and a number of Audit Agents distributed to the various audit source nodes in the network.The PRéCis toolkit operates as a network application, distributed across multiple nodes. The Audit Tools are operated as network clients from the Security Officer’s workstation. They access services provided by the Audit Server component, resident on the PRéCis Server. The Server, which maintains active communications with the entire set of distributed PRéCis components, is the central network component of the PRéCis toolkit and is currently configured to run on a Sun platform.

The Audit Tools software is the set of applications directly supporting the functions performed by the Security Officer. This suite of tools is the Security Officer’s interface to the Toolkit. They support a Motif Graphical User Interface (GUI) and may be operated by the Security Officer from any approved workstation in the network environment, if permitted by your security policy. They can also be operated from the PRéCis Server console. The workstation from which they are operated is called the PRéCis Client. The Audit Tools interact with the Audit Server to obtain information typically for use in audit analysis operations. Through these tools, a Security Officer can query the Audit Analysis data base for normalized audits or query the native audit archive facility for native audits. A Monitor Tool provides a way for the Security Officer to review alerts and significant events on the system. Other analysis tools provide support for recognition of anomalous behavior patterns. Audit Tools also support periodic security assessments and administration and configuration functions necessary for day-to-day operations.

The Audit Server component maintains a central data repository of audits. Normalized audits are placed in the Audit Analysis data base and native audits are archived. The Server supports a client/server interface with the Audit Tools via three classes of services. The Information Management Services provide the Audit Tools with access to the central repository of audits collected from audit source nodes throughout the network. These services also provide the *Virtual Storage* facility



allowing transparent access to the audit archives. The Audit Monitor Services provide anomaly detection facilities, alert processing services, and reporting capabilities– it is through this mechanism that near real-time alerts are processed by the Audit Tools. The third class of service, Configuration Services, supports the maintenance of Audit Agent Configurations.

The Audit Server also supports an agent/manager interface with the Audit Agents. The Agent Interface portion of the Audit Server receives audits sent by the various audit agents and provides a control interface allowing the Audit Server to provide configuration directives to the Audit Agents. Audit Processing functions on the Audit Server provide for data base load and for archiving native audits.

The Audit Server supports near real-time alert notification through unsolicited data feeds to certain Audit Tools. The Audit Server software also supports a manager/agent interface with the Audit Agents distributed throughout the network.

The Audit Agent component is responsible for capturing native audits generated in the network and forwarding them to the Server, where they are processed. Agents are also responsible for converting the native audits into the normalized representation before they are forwarded to the Audit Server. This allows them to screen audits for critical events to be sent immediately to the Server. Audit Agents reside on audit source nodes in the network and are responsible for transporting audits to the PRéCis Server, where the Audit Server Component can archive native audits and load normalized audits into the Audit Analysis data base. In the case where Audit Agents are not configured to perform conversion and reduction, the Audit Server component can be optionally configured to perform this operation on incoming audit streams. However, the trade-off is less timely alert notification.

Agents in the PRC•PRéCis™ product are constructed as generic rule-based agents, capable of operating on multiple types of Unix or Windows NT platforms, working with a variety of audit sources. The agents use a table-based control object allowing them to be tailored to process any audit source. Default tables are provided with the product distribution and can be tailored to process audits according to the security policy at your site. Tables are also used to define rules for the intrusion detection component of the PRéCis toolkit.

Tables are currently available to process Sun OS, SOLARIS, HP-UX, and Windows NT audits.

Litton
PRC

PRC is developing the PRéCis toolkit product to meet the security needs of organizations throughout the DOD and Federal Government. The PRéCis software itself incorporates C2 level safeguards designed to support incremental accreditation of this software in a System High environment.

The PRéCis toolkit will also serve the needs of commercial organizations who wish to take positive steps to protect their valuable information assets from compromise.

PRC welcomes inquiries, comments, or suggestions regarding the planned capabilities of the PRéCis product. For further information, see “Contact Us” page at our website: www.bellevue.prc.com/precis